UCEB

Executive Bulletin

Volume 2, Number 4

Problems Occur When You Can Least Afford Them, So Planning is Critical

With tornadoes in the Midwest, April snows in Colorado, a 6.2 (Richter scale) earthquake in San Jose near the heart of Silicon Valley, and heavy rains in the Northeast and Southeast, it should be obvious to one and all that nature causes disasters from which you, the information system manager, must recover.

The subject of disaster recovery planning, much like insurance, is one that most of us prefer to ignore. This is not because we don't recognize the importance of creating and honoring such a plan, but because we always have other, more time-critical commitments.

This Executive Bulletin will outline key basic items that you should deal with now, in advance of a disaster. Such items include:

1. Storage.
2. Key personnel.
3. Processing facilities.

We at INPUT strongly suggest that you take the time to at least do some basic, preliminary preparation for the "it could never happen to us" disaster, whether it is natural or otherwise. Specifically we suggest that you:

1. Create (and keep current) a method for storing files, programs, documentation, etc.
2. Create (and keep current) a list of key personnel required to keep your company's systems running.
3. Have available (and not only in your desk) as comprehensive a list as possible of local, or near-local, processing facilities, plus the arrangements you (hopefully) have already made with these facilities.

← Add Peter's signature here

File, Data, and Progr

As the one responsible for information system management, your focus should be on the key word--information--without which there is no business. Finding an off-site vault location (at which you can store all of your master files, program listings, processing documentation, et al) is an easy

proposition. (This is different from hiring an off-site Disaster Recovery Service, although if you hire one the problem of off-site storage of critical information and the problem of overall recovery can be handled at one time.) The exact distance this location should be from your operating center is dependent upon the type of major disaster most likely to occur. If, for example, flooding is a possibility then logic dictates that your off-site vault be maintained in a location that is not going to be affected by the same natural catastrophe.

Once you have selected the site, you need to copy and catalog all of the information that should be maintained at this location. Additional copies of this catalog should be kept off-site, preferably at a branch location and at some of the homes of the key personnel. This catalog, and the data that is stored off-site, has to contain all of your "must" systems and as many of your "also important" systems as you can reasonably keep current given the ongoing requirements of your operation.

This leads us to the final point of this section--making sure that, as you back up your system for normal security purposes, you transfer updated master files, necessary transaction files and, if pertinent, new documentation files (or hard copy) to the off-site vault. This ongoing effort must be done at least monthly and should probably be done on a weekly basis to preclude having to manually recreate as much as 30 days worth of transaction data. If a disaster does occur you'll have lots more important things to worry about than catching up with already-completed work.

Key Personnel

If a disaster occurs, the key word to remember is disaster. You will potentially have to process information in a scramble mode. In a worst case situation, you not only can lose your system but some of your key people as well. (This is a gruesome thought, but the contingency must be prepared for.) Other staff members will have to process as much information as they can with limited supervision and decreased processing capabilities.

By maintaining in at least three locations (the vault, on-site, and at the house of one or more staff members) a list of all key personnel, you will still have an ability to process. For each person identified, there should be at least one, preferably two, backup individuals who can support your processing needs. Operations, applications programming, and systems software are the three disciplines that must be protected. Customer support, documentation, data entry, etc. are also important but usually to a lesser degree than these first three.

As a part of this program you need to ensure that all personnel that will be called upon in a disaster are trained in the procedures they will follow. Dry runs, including actually shutting down your system, should be implemented.

If you are a one-shift, one-level-of-staffing shop, you need to consider locating and arranging for a third party to support your system when the need arises. In this case, the key contact information regarding this outside organization should also be kept at the locations mentioned above.

Processing Facilities

You now have the people, the programs, reasonably current updated records, and documentation. All you need now is a computer and a place to run it. Remembering still that disaster is the key word, you will have:

a) Arranged with a sister firm in another locale to support your needs for some period of time. (Remember that these kinds of arrangements are usually reciprocal.)

b) Arranged with a service organization in another location to support you until your installation has recovered.

c) Arranged for a space-only location into which a new hardware configuration can be delivered as soon as your vendor can supply you with the needed equipment.

In addition, you, as part of this requirement, will have a guarantee from your vendor describing how long it will take to get that new system to your space-only backup site or to your new or renovated location.

By covering these three areas, you give yourself primary protection against a disaster putting your organization in an operating bind or, at the very worst, out of business. There are a lot of other items that need to be looked at in order to properly complete a disaster recovery plan, including arrangements for transportation, data entry, communications, supplies, etc. But, by handling the basic three indicated above, you should be able to keep yourself going regardless of the magnitude of the disaster.

And, almost as a by-product, you have begun a formal disaster recovery plan that you should try to complete as soon as you can find the time or get out from under other priorities.

It is in your best interest overall to prepare and fully document a detailed disaster recovery program that at least covers the following items:

- Initial notification procedures.
- Plan organization and structure.
- Plan activation criteria.
- Off-site storage procedures.
- Vault resource requirements listing.
- Software restoration procedures.
- Off-site checklists.
- I/O responsibilities.
  - Critical run reconstruction.
  - Schedules.

- Administrative procedures.
  - Personnel.
  - Security.
  - Transportation.
  - Insurance.
  - PR.
  - Legal.
  - Purchasing/supply.
- User support requirements.
  - Application specialists.
  - User data reconstruction.
  - Critical Data Application Schedules.
  - Special call list.
  - Communications links.
- Testing procedures.
  - Audits.
  - Reviews.

When these, plus others, are completed you will have a full plan—documented, tested, and proven.

Whether you choose to hire an outside service, rent a shell, or rent a full backup facility, you still need the plan and you need to convince senior management that the failure to have such a plan can potentially put you out of business. The availability of a plan can expedite recovery from a disaster as simple as a flood in the computer room or as complex as complete destruction of the machine facility and everything (and everybody) inside.

This Executive Bulletin reminds you that not only does it not pay to fool with Mother Nature, but also it doesn't pay to ignore her.

This INPUT Executive Bulletin is published as part of the Corporate Systems Planning Program of the Information Systems Program. For more information on this bulletin or any other INPUT program, please contact INPUT at 1943 Landings Drive, Mountain View, California 94043, (415) 960-3990.

A REMINDER THAT PROBLEMS OCCUR WHEN YOU CAN LEAST AFFORD THEM BUT WITH TIMELY PLANNING YOU CAN REDUCE THEIR IMPACT

With tornadoes in the Midwest, April snows in Colorado, a 6.2 (Richter scale) earthquake in San Jose near the heart of Silicon Valley, and heavy rains in the Northeast and Southeast, it should be obvious to one and all that nature causes disasters from which you, the information system manager, must recover.

The subject of disaster recovery planning, much like insurance, is one that most of us prefer to ignore. This is not because we don't recognize the importance of creating and honoring such a plan, but because we always have other, more time-critical commitments.

This Executive Bulletin will outline key basic items that you should deal with now, in advance of a disaster. Such items include:

1. Storage.
2. Key personnel.
3. Processing facilities.

We at INPUT strongly suggest that you take the time to at least do some basic, preliminary preparation for the "it could never happen to us" disaster, whether it is

natural or otherwise. Specifically we suggest that you:

1. Create (and keep current) a method for storing files, programs, documentation, etc.
2. Create (and keep current) a list of key personnel required to keep your company's systems running.
3. Have available (and not only in your desk) as comprehensive a list as possible of local, or near-local, processing facilities, plus the arrangements you (hopefully) have already made with these facilities.

File, Data, and Program Storage

As the one responsible for information system management, your focus should be on the key word - information - without which there is no business. Finding an off-site vault location (at which you can store all of your master files, program listings, processing documentation, et al) is an easy proposition. (This is different from hiring an off-site Disaster Recovery Service, although if you hire one the problem of off-site storage of critical information and the problem of overall recovery can be handled at one time.) The exact distance this location should be from your operating center is dependent upon the type of major

disaster most likely to occur. If, for example, flooding is a possibility then logic dictates that your off-site vault be maintained in a location that is not going to be affected by the same natural catastrophe.

Once you have selected the site, you need to copy and catalog all of the information that should be maintained at this location. Additional copies of this catalog should be kept off-site, preferably at a branch location and at some of the homes of the key personnel. This catalog, and the data that is stored off-site, has to contain all of your "must" systems and as many of your "also important" systems as you can reasonably keep current given the ongoing requirements of your operation.

This leads us to the final point of this section - making sure that, as you back up your system for normal security purposes, you transfer updated master files, necessary transaction files and, if pertinent, new documentation files (or hard copy) to the off-site vault. This ongoing effort must be done at least monthly and should probably be done on a weekly basis to preclude having to manually recreate as much as 30 days worth of transaction data. If a disaster does occur you'll have lots more important things to worry about than catching up with already-completed work.

Key Personnel

If a disaster occurs, the key word to remember is disaster. You will potentially have to process information in a scramble mode. In a worst case situation, you not only can lose your system but some of your key people as well. (This is a gruesome thought, but the contingency must be prepared for.) Other staff members will have to process as much information as they can with limited supervision and decreased processing capabilities.

By maintaining in at least three locations (the vault, on-site, and at the house of one or more staff members) a list of all key personnel, you will still have an ability to process. For each person identified, there should be at least one, preferably two, backup individuals who can support your processing needs. Operations, applications programming, and systems software are the three disciplines that must be protected. Customer support, documentation, data entry, etc. are also important but usually to a lesser degree than these first three.

As a part of this program you need to ensure that all personnel that will be called upon in a disaster are trained in the procedures they will follow. Dry runs, including actually shutting down your system, should be implemented.

If you are a one-shift, one-level-of-staffing shop, you need to consider locating and arranging for a third party to support your system when the need arises. In this case, the key contact information regarding this outside organization should also be kept at the locations mentioned above.

Processing Facilities

You now have the people, the programs, reasonably current updated records, and documentation. All you need now is a computer and a place to run it. Remembering still that disaster is the key word, you will have:

a) Arranged with a sister firm in another locale to support your needs for some period of time. (Remember that these kinds of arrangements are usually reciprocal.)
b) Arranged with a service organization in another location to support you until your installation has recovered.
c) Arranged for a space-only location into which a new hardware configuration can be delivered as soon as your vendor can supply you with the needed equipment.

In addition, you, as part of this requirement, will have a guarantee from

your vendor describing how long it will take to get that new system to your space-only backup site or to your new or renovated location.

By covering these three areas, you give yourself primary protection against a disaster putting your organization in an operating bind or, at the very worst, out of business. There are a lot of other items that need to be looked at in order to properly complete a disaster recovery plan, including arrangements for transportation, data entry, communications, supplies, etc. But, by handling the basic three indicated above, you should be able to keep yourself going regardless of the magnitude of the disaster.

And, almost as a by-product, you have begun a formal disaster recovery plan that you should try to complete as soon as you can find the time or get out from under other priorities.

It is in your best interest overall to prepare and fully document a detailed disaster recovery program that at least covers the following items:

- Initial notification procedures.
- Plan organization and structure.
- Plan activation criteria.
- Off-site storage procedures.
- Vault resource requirements listing.
- Software restoration procedures.
- Off-site checklists.

- I/O responsibilities.
  - Critical run reconstruction.
  - Schedules.
- Administrative procedures.
  - Personnel.
  - Security.
  - Transportation.
  - Insurance.
  - PR.
  - Legal.
  - Purchasing/supply.
- User support requirements.
  - Application specialists.
  - User data reconstruction.
  - Critical Data Application Schedules.
  - Special call list.
  - Communications links.
- Testing procedures.
  - Audits.
  - Reviews.

When these, plus others, are completed you will have a full plan--documented, tested, and proven.

Whether you choose to hire an outside service, rent a shell, or rent a full backup facility, you still need the plan and you need to convince senior management that the failure to have such a plan can potentially put you out of business. The availability of a plan can expedite recovery from a disaster as simple as a flood in the computer room or as complex as complete

destruction of the machine facility and everything (and everybody) inside.

This Executive Bulletin reminds you that not only does it not pay to fool with Mother Nature, but also it doesn't pay to ignore her.

This INPUT Executive Bulletin is published as part of the Corporate Systems Planning Program of the Information Systems Program. For more information on this bulletin or any other INPUT program, please contact INPUT at 1943 Landings Drive, Mountain View, California 94043, (415) 960-3990.

A REMINDER THAT PROBLEMS OCCUR WHEN YOU CAN LEAST AFFORD THEM BUT WITH TIMELY PLANNING YOU CAN REDUCE THEIR IMPACT

With tornadoes in the Midwest, April snows in Colorado, a 6.2 ~~on the~~ (Richter scale) earthquake in San Jose near the heart of Silicon Valley, and heavy rains in the Northeast and Southeast, it should be obvious to one and all that nature causes disasters from which you, the information system manager, must recover.

~~Much like the welcome given to an insurance salesperson, which is at best reluctant,~~ The subject of disaster recovery planning, much like insurance, is one that most of us prefer to ignore. This is Not because we don't recognize the importance of creating and honoring such a plan but because we always have other more ~~more pressing,~~ time-critical commitments ~~that fill our time.~~

We at INPUT, strongly suggest, that you take the time to at least do some basic, preliminary preparation for ~~that~~ the "~~never~~ it could never happen to us" ~~event~~ disaster, whether it is naturally or otherwise ~~caused.~~ Specifically we suggest that you:

1. Create (and keep current) a method for storing files, programs, documentation, etc.

Intent: This Executive Bulletin will outline key basic items that you should deal with now in advance of a disaster. ~~including:~~ Such items include:
1. STORAGE
2. KEY PERSONNEL
3. PROCESSING FACILITIES

Format! Introduction should also outline the major sections of the text

2. Create (and keep current) a list of key personnel required to keep your company's systems running.
3. Have available and (not only in your desk) as comprehensive a list as possible of local, or near-local, processing facilities plus the arrangements you (hopefully) have already put in place with them.

Peter Cummings

Is this for Peter C. to see?
No!

File, Data, and Program Storage

As the one responsible for information system management your focus should be on the key word - information - without which there is no business. Finding an off-site vault location at which you can store all of your master files, program listings, processing documentation, et al is an easy proposition. (This is different from hiring an off-site Disaster Recovery Service although if you do this the problem of off-site storage of critical information and the problem of recovery over all can be handled at one time.) The exact distance this location should be from your operating center is dependent upon the type of major disaster most likely to occur. If, for example, flooding is a possibility then logic dictates that your off-site vault be maintained in a location that is not going to be affected by the same natural catastrophe.

ok? or have I changed meaning do this = ?

Once you have selected the site, you need to copy and catalog all of the information that should be maintained at this location. Additional copies of this catalog should be kept off-site, preferably at a branch location and at some of the homes of the key personnel ~~you will call upon to process if, and of course, when a disaster occurs~~. This catalog, and the data that is stored off-site, has to contain all of your "must" systems and as many of your "also important" systems as you can reasonably keep current given the ongoing requirements of your operation.

to process what ?

Which leads us to the final point of this section - making sure that, as you back up your system for normal security purposes, you transfer updated master files, necessary transaction files and, if pertinent, new documentation files (or hard copy) to the off-site vault. This ongoing effort must be done at least monthly and should probably be done on a weekly basis ~~in order~~ to preclude ~~a need to have to~~ having to manually recreate as much as 30 days worth of transaction data. If a disaster does occur you'll have lots more important things to worry about than catching up with already completed work.

Key Personnel

When, or if, a disaster occurs, the key word to remember is disaster. You will potentially have to process information in a scramble mode. In a worst case situation, you not only can lose your system but you can lose some of your key people as well. (Gruesome though, but . . .). This means that other staff members will have to try to process as much of the information as they can with limited supervision and decreased processing capabilities.

(This is a gruesome thought, but the contingency must be prepared for.)

By maintaining a list of all key personnel at at least three locations, the vault, on-site, and at the house of one (or more) staff members, you will have an ability to process. For each person identified, there should be at least one, preferably two, backup individuals indicated who can support your processing needs. Operations, applications programming and systems software are the three disciplines that must be protected - with customer support, documentation, data entry, etc. important but usually to a lesser degree than these first three.

By maintaining in at least three locations, the vault, on-site, and at the house of one or more staff members, you will still have a list of all key personnel, you will still have an ability to process.

something missing here (?) all?

As a part of this program you need to ensure that all personnel ~~that will~~ be called upon in a disaster ~~be~~ trained in the procedures they will follow. Dry runs, including actually shutting down your system, should be implemented ~~(and not only during a time period when the immediacy of the problem is not addressed.)~~

If you are a one-shift, one-level-of-staffing shop, you need to consider locating and arranging for a third party to support your system when the need arises. In this case, the key contact information regarding this outside organization is kept at the locations mentioned above.

Processing Facilities

You now have the people, the programs, reasonably current updated records and documentation. All you need now is a computer and a place to run it. Remembering still that disaster is the key word, you will have:

a) Arranged with a sister firm in another locale to support your needs for some period of time. (Remember that these kinds of arrangements are reciprocal.)
b) Arranged with a service organization in another location to support you until your installation has recovered.

c) Arranged for an space-only location into which a new hardware configuration can be delivered as soon as your vendor can supply you with the needed equipment.

In addition, you, as part of this requirement, will have a guarantee from your vendor describing how long it will take to get that new system to your space-only backup site or to your new or renovated location.

By covering these three areas, you give yourself primary protection against a disaster putting your organization in an operating bind, or at the very worst, out of business. There are a lot of other items that need to be looked ~~at in the proper~~ at in order to properly complete ~~completion of~~ a disaster recovery plan, including arrangements for transportation, data entry, communications, supplies, etc. But, by handling the basic three indicated above, you should be able to keep yourself going regardless of the magnitude of the disaster.

And, almost as a by-product, you have begun a formal disaster recovery plan that you should try to complete as soon as you can find the time or get out from under ~~these~~ other priorities.

It is in your best interest overall to prepare and fully document a detailed disaster recovery program that at least covers the following items:

- Initial notification procedures.
- Plan organization and structure.
- Plan activation criteria.
- Off-site storage procedures.
- Vault resource requirements listing.
- Software restoration procedures.
- Off-site checklists.
- I/O responsibilities.
  - . Critical run reconstruction.
  - . Schedules.
- Administrative procedures.
  - . Personnel.
  - . Security.
  - . Transportation.
  - . Insurance.
  - . PR.
  - . Legal.
  - . Purchasing/supply.
- User support requirements.
  - . Application specialists.
  - . User data reconstruction.
  - . Critical Data Application Schedules.
  - . Special call list.
  - . Communications links.
- Testing procedures.
  - . Audits.
  - . Reviews.

close ups

When these, plus others, are completed you will have a full plan documented, tested, and proven.

Whether you choose to hire an outside service, rent a shell, or rent a full back up facility, you still need the plan and you need to convince senior management that the failure to have such a plan can potentially put you out of business. The availability of a plan can expedite recovery from a disaster as simple as a flood in the computer room to as complex as complete distribution of the machine facility and everything (and person) inside.

This Executive Bulletin is intended to remind you that not only doesn't it not pay to fool with mother nature, it doesn't pay to ignore her either.

The INPUT Executive Bulletin is published as part of the Corporation Systems Planning Program of the Information Systems Program. For more information on this bulletin or any other INPUT program, please contact INPUT at 1943 Landings Drive, Mountain View, California 94043, (415) 960-3990.

This Executive Bulletin reminds you that not only does it not pay to fool with mother nature, but also it doesn't pay to ignore her.

← or Corporate ?

A REMINDER THAT PROBLEMS OCCUR WHEN YOU CAN LEAST AFFORD THEM BUT WITH TIMELY PLANNING YOU CAN REDUCE THEIR IMPACT

With tornadoes in the Midwest, April snows in Colorado, a 6.2 on the Richter scale earthquake in San Jose near the heart of Silicon Valley, heavy rains in the Northeast and Southeast, it should be obvious to one and all that nature causes disasters from which you, the information system manager, must recover.

Much like the unwelcome visit to an insurance salesperson, the subject of disaster recovery planning is one that most of us prefer to ignore. Not because we don't recognise the importance of honoring such a plan but because we always have other more pressing, time-critical commitments that fill our time.

Be that as it may, we at INPUT, strongly suggest, that you take the time to at least do some basic, preliminary preparation for that never happen to us event. Specifically we suggest that you:

1. Create (and keep current) a method for storing files, programs, documentation, etc.
2. Create (and keep current) a list of key personnel required to keep your company's systems running.

3. Have available (not in your desk) as and only
comprehensive a list as possible of
local, or near local, processing
facilities. Plus the arrangements you (hopefully) have already put in place
with them.

File, Data, and Program Storage

As the one responsible for information system management your focus should be on the key word - information - without which there is no business. Finding an off-site vault location at which you can store all of your master files, program listings, processing documentation, et al is an easy proposition. The exact distance this location should be from your operating center is dependent upon the type of major disaster most likely to occur. If, for example, flooding is a possibility then logic dictates that your off-site vault be maintained in a location that is not going to be affected by the same natural catastrophe.

(This is different from hiring an off-site disaster recovery service although if you do this the problem of off-site storage of critical information and the problem of recovery can be handled at one time.)

Once you have selected the site, you need to copy and catalog all of the information that should be maintained at this location. Additional Copies of the catalog should be kept off site, preferably at a branch location and at some of the homes of the key personnel you will call upon to process when a disaster occurs. This catalog, and the data that is stored off site, must contain all of your "must" systems and as many of your "when needed" systems as you can reasonably keep current. GIVEN the ongoing requirements of your operation.

Which leads us to the final point of this section - making sure that, as you back up your system for normal security purposes, you transfer updated master files, necessary transaction files and, if pertinent, new documentation files (or hard copy) to the vault. This ongoing effort ~~should~~ MUST be done at least monthly and probably SHOULD BE DONE on a weekly basis in order to preclude a need to have to manually recreate as much as 30 days worth of transaction data. IF A DISASTER DOES OCCUR you'll HAVE LOTS MORE IMPORTANT THINGS TO WORRY ABOUT THAN CATCHING UP WITH ALREADY COMPLETED WORK.

OFF-SITE

Key Personnel

When, or if, a disaster occurs, the key word (~~not information, this time~~) to remember is disaster. You will potentially have to process information in a scramble mode, IN a worst case situation, you not only can lose your system but your key people as well. (AWESOME THOUGHT, — BUT ---) This means that other staff members will have to try to process as much of the information they can with limited supervision and decreased processing capabilities.

CAN LOSE SOME OF YOUR

By maintaining a list of all key personnel at at least three locations, the vault, on-site, and at the house of one (or more) staff members, you will have an ability to process. For each person identified, there should be at least one, preferably two, back-up individuals

indicated who can support your processing needs. Operations, applications programming and systems software are the three disciplines that must be protected with customer support, documentation, data entry, etc. important but ~~probably~~ USUALLY TO A LESSER DEGREE ~~less so~~ than these first three.

as a part of this program you need to ensure that all personnel that will be called upon in a disaster be trained in the procedures they will follow. Day runs, including actually shutting down your system, should be implemented. (and not only during a time period ~~third shift~~ when the immediacy of the problem is not addressed.)

If you are a one-shift, one level of staffing shop, you need to consider locating and arranging for a third party to support your system ~~is~~ WHEN the need arises. ~~For~~ IN this case, the key contact INFORMATION ~~[illegible]~~ REGARDING ~~for~~ this outside organization is kept at the locations mentioned above.

Processing Facilities

You now have the people, the programs, reasonably current updated records and documentation. All you need is NOW a COMPUTER AND A place to run IT. Remembering still that disaster is the key word, you will have:

a) ARRANGED with a sister firm in another locale to support your needs for some period of time. (Remember that these kinds of arrangements are RECIPROCAL.)

b) ARRANGED with a service organization in another location to support you until your installation has recovered.

c) ARRANGED for an space-only location into which a new hardware configuration can be delivered as soon as your vendor can ~~do so~~ SUPPLY YOU WITH THE NEEDED EQUIPMENT

In addition, you, as part of this requirement, will have a guarantee from your vendor describing how long it will take to get that new system to your space-only backup site or to your new or renovated location.

~~Now that wasn't all that difficult.~~ By covering these three areas, you give yourself primary protection against a disaster putting your organization in an OPERATING BIND, or ATTREVERY worse, out of business. There are a lot of other items that need to be looked at in the proper completion of a disaster RECOVERY PLAN INCLUDING ARRANGEMENTS FOR: transportation, data entry, communications, supplies, etc. But, by handling the basic three INDICATED ABOVE, you should be able to keep yourself going regardless of the magnitude of the disaster.

And, ALMOST AS A BY PRODUCT, you have begun a FORMAL disaster recovery plan, that you should TRY TO complete as soon as you can find the time or get out from under those other priorities.

This Executive Bulletin is intended to remind you that not only doesn't it not pay to fool with mother nature, it doesn't pay to ignore her either.

*Insert ①

This INPUT Executive Bulletin is published as part of the Corporation Systems Planning Program of the Information Systems Program. For more information on this bulletin or any other INPUT Program, please contact INPUT AT 1943 Landings Drive, Mountain View, California, 94043, (415) 960-3990.

~~ANSWER~~

Insert 1

~~Of course~~ It is in your best interest overall to prepare and fully document a detailed disaster recovery program that at least covers the following items:

- initial notification procedures
- Plan organization and structure
- Plan activation criteria
- Off-site storage procedures
- Vault resource requirements listing
- Software restoration procedures
- Off-site checklists
- I/O responsibilities
- Critical run reconstruction (SUBSET under I/O)
- Schedules
- ADMINISTRATIVE procedures
  - personnel
  - Security
  - Transportation
  - Insurance
  - PR
  - Legal
  - Purchasing/Supply
- User support requirements
  - Application Specialists
  - User data reconstruction

- Critical Data Application Schedules
- Special call list
- Communications Links

– Testing procedures
  - AUDITS
  - REVIEWS

(NOT) When these, plus others, are completed you will have a full plan, documented, tested and proven. Whether you choose to hire an outside service, rent a shell, or rent a full back up facility, you still need the plan and you need to convince senior management that the failure to have such a plan can potentially put you out of business. The availability of ~~th~~ a plan can expedite recovery from a disaster as simple as a flood in the computer room to as complex as complete destruction of the machine facility and everything (and person) inside.

U-CEB BACKUP

Executive Bulletin

Volume 2, Number 3

An Unusually Noteworthy Introduction of a Xenolith*

Eight years ago, INPUT predicted a battle between two giants as computer and communications technologies merged into integrated networks. Since then, IBM revenue has grown from $16 billion to $40 billion, and the Bell System has been broken up. From a hardware point of view, AT&T Technologies Inc.'s announcement of its 3B line of 32-bit processors is strictly David versus Goliath, but David's sling is armed with a xenolith aimed directly at Goliath's software monolith. The UNIX shot was telegraphed from way back, and Goliath looks bored by these developments; but we have all been waiting for this match, so let's take a look at it.

1. The Target is Right!
2. SNA Xenophobia
3. VM/CMS/MVS/XA/UNIX - Excalibur?

The Target is Right!

INPUT predicted the IBM-AT&T battle in the Economics of Computer/Communications Networks and Their Future Impact, March 1976. That report also described hierarchical networks consisting of very large mainframes ($4 million price range), minicomputers (less than $200,000), and intelligent terminals (less than $20,000) and defined their "proper functions" as follows:

- Mainframes - heavy computation, transaction processing against large data bases, and RJE replacement of standalone batch systems.
- Minicomputers - network control, scientific timesharing, program development and maintenance, and simple transaction processing.
- Intelligent Terminals - collection, editing, and display of data; control of lower level terminals (input-output devices).

* Xenolith - A fragment of rock included in another rock

In a brief analysis of IBM's then recently announced Systems Network Architecture (SNA), INPUT stated: ". . .there is little indication that IBM either understands or has any intention of implementing networks incorporating multifunction Level IIs (minicomputers). . ." In the last eight years, INPUT has seen no reason to revise this opinion. IBM has used SNA as a means of excluding minis (including their own Series 1) from their "proper" (and cost-effective) place in the processing hierarchy. However, the advantages of minicomputers for the communications-oriented, interactive functions assigned to them have become apparent, and growth in the use of minicomputers has substantially impacted general mainframe growth.

All of IBM's alternatives to the use of minicomputers (from large host processing down through the relatively recent announcements of the 4361 and XT/370) suffer from the same problem - they must compete, burdened by software that was not specifically designed for the communications-oriented, interactive environment in which minicomputers thrive.

David seems to have adopted a rather clever strategy. During the first round he has targeted a hardware area where Goliath has seen fit to avoid one-on-one combat. In fact, David may knock over a few of Goliath's smaller minicomputer tormentors while in the process of directing his UNIX xenolith at Goliath's softest spot - software. However, David may find even Goliath's soft spot difficult to penetrate.

SNA Xenophobia

One analyst reacted to the 3B series announcement with the statement: "High tech, high price." And, in fact, the prices of the high-end 3B205, A & D ($230,000 to $340,000) seem aimed more at the IBM 4361 and 4381 mainframes than they are at the Data General and DEC lines of superminis (which still fall below INPUT's $200,000 definition for minicomputers). However, it should not necessarily be assumed that David has missed the target completely.

- The 3B series is aimed at the office and local area networks. Two Ethernet-compatible interfaces are provided, but 3B Net is reported to have five times the throughput of current Ethernet-type LANs with significantly less burden on the attached processors.

- The processors are stated to be twice as reliable as other commercially available computers (10 minutes downtime per year) and operate within a temperature range of 32°F to 122°F.

- In fact, the 3B20 (as specified) is more like the #5 ESS switching systems than it is a conventional minicomputer. As such, its life expectancy is probably projected to be longer than commercially available minicomputers and most certainly longer than IBM mainframes where planned obsolescence is the order of the day.

- The extended life, plus performance under UNIX, should result in a relatively cheap cost when measured on the basis of cost per terminal over the life cycle. Office systems are communications systems, and it should be hoped that their reliability, performance, and effective life will more closely parallel those of communications networks rather than data processing systems.

The 3B5/100 and 200 are based on a 32-bit microprocessor developed by AT&T's Technology Systems Group. They are classified as "mid-range superminis," are purported to be optimized for UNIX, support 30 and 60 users respectively, and sell for between $57,000 and $73,000. The 3B2/300 (based on the same microprocessor) is a desktop unit that sells for $9,500, supports up to 18 users, and later this year will provide a UNIX host for personal computers (IBM PC and compatibles) including an anticipated 3BX personal computer.

The 3B line is a well-planned, high-quality, hardware/software system from the only vendor with a chance to match Goliath's reputation - but it all depends on UNIX. An AT&T spokesperson has stated that the announcement of UNIX System V has moved it "beyond academics and technical gurus." Perhaps this is true, but when one of the 10,000 marketing representatives AT&T plans to employ by the end of the year (a major challenge in its own right) calls on a typical IBM, SNA-oriented IS department, the rep is likely to find a xenophobe who views both the rep and the xenolith as something from outer space.

VM/CMS/MVS/XA/UNIX - Excalibur?

However, David's first shot may hit the target among some of Goliath's most valued customers - those large enough and advanced enough to push the state-of-the-art in networks. In that case, Goliath may be temporarily stunned and the fight may proceed to round two. Then David will be armed with a UNIX sword rather than a mere sling and stone. Even though Goliath may be reduced from giant to king size, you

can be sure he will have the strength to wrest the sword from David and embed it firmly in the solid, unfathomable IBM software monolith.

UNIX will become just a part (and from IBM's point of view, a minor part) of the greater VM/CMS/MVS/XA whole. IBM's agreement with Computervision for the development of a 4300-based CAE/CAD/CAM system under VM/CMS and the SQL/DS relational DBMS, using UNIX only at the intelligent workstation level, will give some idea of how deeply IBM would prefer to push the sword into the stone. However, UNIX could be run as "just another operating system" under VM at any level. Thus will the challenge be laid down during round two, and it will remain to be seen whether David can turn into Arthur and wrest Excalibur from the stone in order to fight another round.

In the meantime, the combined hardware/software implications of the announcement must be analyzed because of their potential impact on network architecture, performance, and productivity. The INPUT research program for this year provides in-depth coverage of all of these areas.

This INPUT Executive Bulletin is published as part of the Corporate Systems Planning Program of the Information Systems Program. For more information on this bulletin, or on this or any other INPUT program, contact INPUT at 1943 Landings Drive, Mountain View, California 94043, (415) 960-3990.

Executive Bulletin

Volume 2, Number 3

An Unusually Noteworthy Introduction of a Xenolith*

Eight years ago, INPUT predicted a battle between two giants as computer and communications technologies merged into integrated networks. Since then, IBM revenue has grown from $16 billion to $40 billion, and the Bell System has been broken up. From a hardware point of view, AT&T Technologies, Inc.'s announcement of its 3B line of 32-bit processors is strictly David versus Goliath, but David's sling is armed with a xenolith aimed directly at Goliath's software monolith. The UNIX shot was telegraphed from way back, and Goliath looks bored by these developments, but we have all been waiting for this match, so let's take a look at it.

1. The Target is Right!

2. SNA Xenophobia

3. VM/CMS/MVS/XA/UNIX - Excalibur?

The Target is Right!

INPUT predicted the IBM-AT&T battle in the Economics of Computer/Communications Networks and Their Future Impact, March 1976. That report also described hierarchical networks consisting of very large mainframes ($4 million price range), minicomputers (less than $200,000), and intelligent terminals (less than $20,000) and defined their "proper functions" as follows:

- Mainframes - heavy computation, transaction processing against large data bases, and RJE replacement of standalone batch systems.

- Minicomputers - network control, scientific timesharing, program development and maintenance, and simple transaction processing.

- Intelligent Terminals - collection, editing, and display of data; control of lower level terminals (input-output devices).

* Xenolith - A fragment of rock included in another rock

In a brief analysis of IBM's then recently announced Systems Network Architecture (SNA), INPUT stated: "...there is little indication that IBM either understands or has any intention of implementing networks incorporating multifunction Level IIs (minicomputers)..." In the last eight years, INPUT has seen no reason to revise this opinion. IBM has used SNA as a means of excluding minis (including their own Series 1) from their "proper" (and cost-effective) place in the processing hierarchy. However, the advantages of minicomputers for the communications-oriented, interactive functions assigned to them have become apparent, and growth in the use of minicomputers has substantially impacted general mainframe growth.

All of IBM's alternatives to the use of minicomputers (from large host processing down through the relatively recent announcements of the 4361 and XT/370) suffer from the same problem - they must compete, burdened by software that was not specifically designed for the communications-oriented, interactive environment in which minicomputers thrive.

David seems to have adopted a rather clever strategy. During the first round he has targeted a hardware area where Goliath has seen fit to avoid one-on-one combat. In fact, David may knock over a few of Goliath's smaller minicomputer tormentors while in the process of directing his UNIX xenolith at Goliath's softest spot - software. However, David may find even Goliath's soft spot difficult to penetrate.

SNA Xenophobia

One analyst reacted to the 3B series announcement with the statement: "High tech, high price." And, in fact, the prices of the high-end 3B205, A & D ($230,000 to $340,000) seem aimed more at the IBM 4361 and 4381 mainframes than they are at the Data General and DEC lines of superminis (which still fall below INPUT's $200,000 definition for minicomputers). However, it should not necessarily be assumed that David has missed the target completely.

- The 3B series is aimed at the office and local area networks. Two Ethernet-compatible interfaces are provided, but 3B Net is reported to have five times the throughput of current Ethernet-type LANs with significantly less burden on the attached processors.

- The processors are stated to be twice as reliable as other commercially available computers (10 minutes downtime per year) and operate within a temperature range of 32°F to 122°F.

- In fact, the 3B20 (as specified) is more like the #5 ESS switching systems than it is a conventional minicomputer. As such, its life expectancy is probably projected to be longer than commercially available minicomputers and most certainly longer than IBM mainframes where planned obsolescence is the order of the day.

- The extended life, plus performance under UNIX, should result in a relatively cheap cost when measured on the basis of cost per terminal over the life cycle. Office systems are communications systems, and it should be hoped that their reliability, performance, and effective life will more closely parallel those of communications networks rather than data processing systems.

The 3B5/100 and 200 are based on a 32-bit microprocessor developed by AT&T's Technology Systems Group. They are classified as "mid-range superminis," are purported to be optimized for UNIX, support 30 and 60 users respectively, and sell for between $57,000 and $73,000. The 3B2/300 (based on the same microprocessor) is a desktop unit that sells for $9,500, supports up to 18 users, and later this year will provide a UNIX host for personal computers (IBM PC and compatibles) including an anticipated 3BX personal computer.

The 3B line is a well-planned, high-quality, hardware/software system from the only vendor with a chance to match Goliath's reputation - but it all depends on UNIX. An AT&T spokesperson has stated that the announcement of Unix System V has moved it "beyond academics and technical gurus." Perhaps, but when one of the 10,000 marketing representatives AT&T plans to employ by the end of the year (a major challenge in its own right) calls on a typical IBM, SNA-oriented IS department, the rep is likely to find an xenophobe who views both them and their xenolith as something from outer space.

VM/CMS/MVS/XA/UNIX - Excalibur?

However, David's first shot may hit the target among some of Goliath's most valued customers - those large enough and advanced enough to push the state-of-the-art in networks. In that case, Goliath may be temporarily stunned and the fight may proceed to round two. Then David will be armed with a UNIX sword rather than a mere sling and stone. Even though Goliath may be reduced from giant to king size, you

can be sure he will have the strength to wrest the sword from David and embed it firmly in the solid, unfathomable IBM software monolith.

UNIX will become just a part of the greater VM/CMS/MVS/XA whole (and hopefully, from IBM's point of view, a minor part). IBM's agreement with Computervision for the development of a 4300-based CAE/CAD/CAM system under VM/CMS and the SQL/DS relational DBMS, using UNIX only at the intelligent workstation level, will give some idea of how deeply IBM would prefer to push the sword into the stone. However, UNIX could be run as "just another operating system" under VM at any level. Thus will the challenge be laid down during round two, and it will remain to be seen whether David can turn into Arthur and wrest Excalibur from the stone in order to fight another round.

In the mean time, the combined hardware/software implications of the announcement must be analyzed because of their potential impact on network architecture, performance, and productivity. The INPUT research program for this year provides in-depth coverage of all of these areas.

This INPUT Executive Bulletin is published as part of the Corporate Systems Planning Program of the Information Systems Program. For more information on this bulletin, or on this or any other INPUT program, contact INPUT at 1943 Landings Drive, Mountain View, California 94043, (415) 960-3990.

AN UNUSUALLY NOTEWORTHY INTRODUCTION OF A XENOLITH *

Eight years ago, INPUT predicted a battle between two giants as computer and communications technologies merged into integrated networks. Since then, IBM revenue has grown from $16 billion to $40 billion, and the Bell System has been broken up. From a hardware point-of-view, ~~the~~ AT&T Technologies, Inc.'s announcement of its 3B line of 32-bit processors is strictly David versus Goliath, but David's sling is armed with an xenolith aimed directly at Goliath's software monolith. The UNIX shot was telegraphed form way back, and Goliath looks ~~practically bored~~ bored by these developments, but we have all been waiting for this match, so let's take a look at it.

1. The Target is Right!

2. SNA Xenophobia

3. VM/CMS/MVS/XA/UNIX - Excalibur?

* Xenolith = A fragment of rock included in another rock

The Target is Right!

INPUT predicted the IBM-AT&T battle in the Economics of Computer/Communications Networks and Their Future Impact, March 1976. That report also described hierarchical networks consisting of very large mainframes ($4 million price range), minicomputers (less than $200,000), and intelligent terminals (less than $20,000) and defined their "proper functions" as follows:

- Mainframes - heavy computation, transaction processing against large data bases, and RJE replacement of standalone batch systems.

- Minicomputers - network control, scientific timesharing, program development and maintenance, and simple transaction processing.

- Intelligent Terminals - collection, editing, and display of data; ~~and~~ & control of lower level terminals (input-output devices).

In a brief analysis of IBM's then recently announced Systems Network

Architecture (SNA), INPUT stated: "...there is little indication that IBM either understands or has any intention of implementing networks incorporating multifunction Level IIs (minicomputers) ..." In the last eight years, INPUT has seen no reason to revise this opinion. IBM has used SNA as a means of excluding minis (including their own Series I) from their "proper" (and cost-effective) place in the processing hierarchy. However, the advantages of minicomputers for the communications-oriented, interactive functions assigned to them have become apparent, and growth in the use of minicomputers has substantially impacted general mainframe growth.

All of IBM's alternatives to the use of minicomputers (from large host processing down through the relatively recent announcements of the 4361 and XT/370) suffer from the same problem - they must compete burdened by software which was not specifically designed for the communications-oriented, interactive environment in which minicomputers thrive.

David seems to have adopted a rather clever strategy. During the first round he has targeted a hardware area where Goliath has seen fit to avoid one-on-one combat. In fact, David may punch out a few of

Goliath's smaller minicomputer tormentors while in the process of directing his UNIX ~~xenolity~~ xenolith at Goliath's ~~most tender~~ softest spot - software. However, David may find even Goliath's soft spot difficult to penetrate.

SNA Xenophobia

One analyst reacted to the 3B series announcement with the statement: "High tech, high price." And, in fact, the prices of the high end 3B205, A & D ($230,000 to $340,000) seem aimed more at the IBM 4361 and 4381 mainframes than they are at the Data General and DEC lines of superminis (which still fall below INPUT's $200,000 definition for minicomputers). However, it should not necessarily be assumed that David has missed the target completely.

- The 3B series is aimed at the office and local area networks. Two Ethernet-compatible interfaces are provided, but 3B Net is reported to have five times the throughput of current Ethernet-type LANs with significantly less burden on the attached processors.

- The processors are stated to be twice as reliable as other

commercially available computers (10 minutes downtime per year) and operate within a temperature range of 32°F to 122°F.

- In fact, the 3B20 (as specified) is more like the #5 ESS switching systems than it is a conventional minicomputer. As such, it's life expectancy is probably projected to be longer than commercially available minicomputers and most certainly longer than IBM mainframes where planned obsolescence is the order of the day.

- The extended life, plus performance under UNIX, should ~~give~~ result in a relatively cheap cost when measured on the basis of cost per terminal over the life cycle. Office systems are communications systems, and it should be hoped that their reliability, performance, and effective life will more closely parallel those of communications networks rather than data processing systems.

The 3B5/100 and 200 are based on a 32-bit microprocessor developed by AT&T's Technology Systems Group. They are classified as "mid-range superminis," are purported to be optimized for UNIX, support 30 and 60 users respectively, and sell for between $57,000 and $73,000. The 3B2/300 (based on the same microprocessor) is a desktop unit which sells for $9,500, supports up to 18 users, and later this year will provide a UNIX host for personal computers (IBM PC and compatibles) including an anticipated 3BX personal computer.

The 3B line is a well-planned, high-quality, hardware/software system from the only vendor with a chance to match Goliath's reputation, but it all depends on UNIX. An AT&T spokesman has stated that the announcement of Unix System V has moved it "beyond academics and technical gurus." Perhaps, but when one of the 10,000 marketing representatives AT&T plans to employ by the end of the year (a major challenge in its own right) calls on a typical IBM, SNA-oriented IS department, he is likely to find an xenophobe who views both him and his xenolith as something from outer space.

VM/CMS/MVS/XA/UNIX - Excalibur?

However, David's first shot may hit the target among some of Goliath's most valued customers - those large enough and advanced enough to push the state-of-the-art in networks. In that case, Goliath may be temporarily stunned and the fight may proceed to round two. Then David will be armed with a UNIX sword rather than a mere sling and stone. Even though Goliath may be reduced from giant to king size, you can be sure he will have the strength to wrest the sword from David and implant it firmly in the solid, unfathomable IBM software monolith.

UNIX will become just a part of the greater VM/CMS/MVS/XA whole (and hopefully from IBM's point-of-view a minor part). IBM's agreement with Computervision for the development of a 4300-based CAE/CAD/CAM system under VM/CMS and the SQL/DS relational DBMS, using UNIX only at the intelligent workstation level will give some idea of how deeply IBM would prefer to push the sword into the rock. However, UNIX could be run as "just another operating system" under VM at any level. Thus will the challenge be laid down during round two, and it will remain to be seen whether David can turn into Arthur and wrest Excalibur

from the ~~rock~~ stone in order to fight another round.

In the mean time, the combined hardware/software implications of the announcement must be analyzed because of ~~its~~ their potential impact on network architecture, performance, and productivity. The INPUT research program for this year provides in-depth coverage of all of these areas.

UCEB ①

~~EB... ??~~

An Unusually Noteworthy Introduction of a Xenolith

Eight years ago, INPUT predicted a battle between two giants ~~[illegible]~~ as computer and communications technologies merged ~~into~~ into integrated networks. Since then, IBM revenue has grown from ~~[illegible]~~ $16 billion to $40 billion, and the Bell System has been broken up. From a hardware point-of-view, the AT&T Technologies, Inc. announcement of ~~the~~ its 3B line of 32-bit processors is ~~[illegible]~~ strictly David versus Goliath, but David's sling is armed with an xenolith aimed directly at Goliath's software monolith. ~~[illegible]~~ ~~blush~~ The UNIX shot was telegraphed from way back, ~~[illegible]~~ and Goliath looks practically bored, but we have all been waiting for this match, so let's take a look at it.

1 - The Target is Right!

2 - ~~Follow~~ SNA Xenophobia

~~[illegible]~~

3 - VM/(CMS/MVS)/XA/UNIX – Excalibur ?

end Page 1

The Target is Right!

INPUT predicted the IBM - AT&T battle in the Economics of Computer/Communications Networks and their Future Impact, March 1976. That report described ~~a~~ hierarchical networks consisting of very large mainframes ($4 million price range), minicomputers (< $200,000) and intelligent terminals (< $20,000) ~~and other terminals~~ and defined their "proper functions" as follows:

- Mainframes - heavy computation, transaction processing against large data bases, and RJE replacement of standalone batch systems.

- Minicomputers - network control, scientific timesharing, program development & maintenance, and simple transaction processing.

– Intelligent Terminals – collection, editing and display of data; and control of lower level terminals (input-output devices).

In a brief analysis of IBM's then recently announced Systems Networks Architecture (SNA), INPUT stated: "... there is little indication that IBM either understands or has any intention of implementing networks incorporating multifunction Level II's (minicomputers) ...". In the last eight years, INPUT has seen no reason to revise this opinion. IBM has used SNA as a means of excluding mini's (including their own Series 1) from their "proper" (and cost effective) place in the processing hierarchy. However, the advantages of minicomputers for the communications oriented, interactive functions assigned to them have become apparent, and growth in the use of minicomputers has substantially impacted general mainframe growth.

All of IBM's alternatives to the use of minicomputers (from large host processing down through the relatively recent announcements of the 4361 and XT/370) suffer from the same problem – they must compete burdened by software which was not specifically designed for the communications-oriented, interactive environment in which minicomputers thrive.

David seems to have adopted a rather clever strategy. During the first round he has targeted a hardware area where Goliath has seen fit to avoid one-on-one combat. In fact, David may punch out a few of Goliath's smaller minicomputer tormentors while in the process of directing his UNIX xenolith at Goliath's most tender spot – software. However, David may find even Goliath's soft spot difficult to penetrate.

2- SNA Xenophobia

One analyst reacted to the 3B series announcement with the statement: "High tech, high price." And, in fact, the pricing of the high end 3B20S, A & D ($230,000 to $340,000) seem aimed more at the IBM

4361 and 4381 mainframes than they ~~are~~ are at the Data General and DEC lines of superminis ~~that~~ (which still fall below INPUT's $200,000 definition for minicomputers). ~~Perhaps it would~~ However, it should not necessarily be assumed that David has missed the target completely.

- The 3B series is aimed at the office and local area networks. Two Ethernet-compatible interfaces are provided, but 3BNet is reputed to have five times the throughput of current Ethernet-type LAN's with significantly less burden on the attached processors.

- The processors are stated to be three as reliable as other commercially available computers (10 minutes downtime per year) and operate within a temperature range of 32°F to 122°F.

- In fact, the 3B20 as specified is more like the #5 ESS switching systems than it is a conventional minicomputer. As such, it's life expectancy ~~is~~ is probably projected to be longer than commercially available minicomputers and most certainly longer than IBM mainframes, where planned obsolescence is the order of the day.

– The extended life, plus performance under UNIX, (~~the processors are purported to maximize UNIX performance~~) ~~will~~ should give relatively cheap cost when measured on the basis of cost per terminal over the life cycle. ~~Once the office~~ → Office systems are communications systems, and it should be hoped that their reliability, ~~and~~ performance and effective life will more closely parallel those of communications networks rather than data processing systems.

The 3B5/100 & 200 ~~& 300~~ are based on a 32-bit microprocessor developed by AT&T's Technology Systems Group. They are classified as "mid-range superminis", are purported to be optimized for UNIX, support 30 & 60 users respectively, and sell for between $57,000 and $73,000. The 3B2/300 (based on the same microprocessor) is ~~classified as~~ a desktop unit which sells for $9,500, supports up to 18 users, and later this year will provide a UNIX host for personal computers (IBM PC & compatibles) including an anticipated 3BX personal computer.

~~It~~ The ~~entire~~ 3B line ~~[illegible]~~ is a well planned, high quality, hardware/software system from the only vendor with a chance to match Goliaths reputation, but it all depends on ~~the Unix [illegible]~~ UNIX. An AT&T spokesman has stated that the announcement of Unix System V has moved it "beyond academics and technical gurus." Perhaps, but when one of the 10,000 marketing ~~personnel~~ representatives AT&T plans to employ by the end of the year (a major challenge in its own right) ~~called~~ calls on a typical IBM, SNA-oriented IS department, he is likely to find an xenophobe who views both him and his xenolith as something from outer space.

3 - VM/CMS/MVS/XA/UNIX - Excalibur?

~~However, among the more advanced~~

However, David's first shot may hit the target among some of Goliaths most valued customers - those large enough and advanced enough to push the state-of-the-art in networks. In that case, Goliath may be temporarily stunned and the fight may

proceed to round two. Then David will be armed with a UNIX sword rather than a sling and stone. Even though Goliath may be reduced from giant to hing size you can be sure he will have the strength to wield the sword from David and implant it firmly in the solid, unfathomable IBM software monolith.

UNIX will become just a part of the greater VM/CMS/MVS/XA whole (and hopefully from IBM's point-of-view a minor part). IBM's agreement with Computervision for the development of a 4300 based CAE/CAD/CAM system under VM/CMS and to SQL/DS relational DBMS, using UNIX only at the intelligent workstation level will give some idea of how deeply IBM would prefer to push the sword into the rock. However UNIX could be run as "just another" operating system" under VM at any level. Thus will the challenge be laid down during round two, and it will remain to be seen whether David can turn into Arthur and wrest Excalibur from the rock in order to fight another round.

In the mean time, the combined hardware/software implications of the announcement must be analyzed because of its potential impact on network architectures, performance, and productivity. The INPUT research program for this year provides in-depth coverage of all of these areas.